23

⑦ Heights

$\rightsquigarrow$ key tool to prove the finiteness of Prep (f, K) over a number field (thm B)

idea = measure of the complexity of a point in $\bar{\mathbb{Q}}$
notion that was formalized by A. Weil when proving Mordell–Weil theorem

$x \in \mathbb{Q}$ $\quad x = \frac{a}{b}$ $\quad a \wedge b = 1$ $\quad h(x) \overset{def}{=} \operatorname{Log} \max |a|, |b|$

up to a constant = # of digits needed to write x.

~~Using the results of the previous chapter~~, I shall now explain how to extend h to $\mathbb{Q}^{alg}$.

idea! $x \in \mathbb{Q}^{alg}$

$P(T) = a_0 T^d + \dots + a_d$ minimal polynomial $\in \mathbb{Z}[T]$.

$\gcd(a_0, a_1, \dots a_d) = 1$

set $\bar{h}(x) = \frac{1}{d} \operatorname{Log} \max |a_i|$

Fact

① $\bar{h}(x) = h(x)$ if $x \in \mathbb{Q}$.

② $\bar{h}(\sigma(x)) = \bar{h}(x)$ for any $x \in \mathbb{Q}^{alg}$, $\sigma \in \mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q})$.

③ N, H finite $\mathcal{E} = \{x \in \mathbb{Q}^{alg},\ [\mathbb{Q}(x) : \mathbb{Q}] \leq N$, $\bar{h}(x) \leq H\}$ is finite

proof ① & ② !

③ $x \in \mathcal{E}$ satisfies $a_0 x^d + \dots + a_d = 0$ $\quad \underset{\mathbb{Z}}{|a_i|} \leq (e^H)^d$

$(2(e^H)^d + 1)^{d+1}$ possible polynomials ///

2/

$\rightsquigarrow$ $\overline{R}$ is easy to compute but hard to relate to deeper arithmetic properties.

idea 2 use the product formula.

~~[illegible]~~

Observation $x \in \mathbb{Q}$.

$$h(x) = \sum_{v \in M_{\mathbb{Q}}} \operatorname{Log}^+ |x|_v \qquad \operatorname{Log}^+ = \max\{0, \operatorname{Log}\}.$$

proof. $x = \prod_{p \in \mathcal{P}} x^{v_p(x)}$ $\quad v_p(x) \in \mathbb{Z}$ $\quad v_p(x) = 0$ for all but finitely many primes.

$$h(x) = \max\Big\{ \sum_{v_p(x) > 0} v_p(x) \operatorname{Log}(p), \sum_{v_p(x) < 0} -v_p(x) \operatorname{Log}(p) \Big\}.$$

$$H(x) = \sum_{v \in M_{\mathbb{Q}}} \operatorname{Log}^+ |x| = \operatorname{Log} \max\{1, |x|_\infty\} - \sum_{v_p(x) < 0} v_p(x) \operatorname{Log}(p)$$

///

def $x \in K$ number field.

$$h_K(x) \overset{\text{def}}{=} \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \operatorname{Log}^+ |x|_v. \qquad n_v = [K_v : \mathbb{Q}_v]$$

Prop ~~[illegible]~~

- $h_K(x) = h(x)$ if $x \in \mathbb{Q}$
- Fix $K \hookrightarrow \mathbb{C}_v$ for each $v \in M_{\mathbb{Q}}$. ($\mathbb{C}_\infty = \mathbb{C}$!)

$$h_K(x) = \frac{1}{\deg(x)} \sum_{v \in M_{\mathbb{Q}}} \sum_{y \in \mathbb{C}_v} \operatorname{Log}^+ |y|_v$$

Galois conjugate of x.

obs: h is well-defined on $\overline{\mathbb{Q}}$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant.

proof.

① !

②. Fix a place $p \in M_{\mathbb{Q}}$. Recall there are exactly $n = [K:\mathbb{Q}]$ embeddings of K into $\mathbb{C}_p$ $(\sigma_1 \dots \sigma_n)$ and for each $v \in M_{K,p}$ $\#\{i,\ |\sigma_i| = |\cdot|_v\} = n_v$.

$x \in K$

$$\sum_v n_v \log^+|x|_v = \sum_i \log^+|\sigma_i(x)| = [K:\mathbb{Q}[x]] \sum_{\substack{y \in \mathbb{C}_p \\ \text{Gal conj} \\ \text{of } x}} \log^+|y|$$

///

$$[K:\mathbb{Q}] = \underbrace{[\mathbb{Q}:\mathbb{Q}(x)]}_{\deg(x)}\,[K:\mathbb{Q}[x]]$$

$\boxed{\text{Thm}}$ N, H fixed $\mathcal{E} = \{x \in \overline{\mathbb{Q}},\ [\mathbb{Q}(x):\mathbb{Q}] \le N,\ h(x) \le H\}$ is finite.

proof $x \in \mathcal{E}$

$f(T) = T^d + a_1T^{d-1} + \dots + a_d$. minimal polynomial $a_i \in \mathbb{Z}$ $\gcd(a_i) = 1$

$= \prod_{i=1}^{d} (T - y_i)$.

a_i = symmetric polynomial $(y_1 \dots y_d)$ = homogeneous of degree i

$v \in M_{\mathbb{Q}}$ $\max\{1, |a_i|_v\} \le C'_{d,v} \max\{1, |y_1|_v, \dots, |y_d|_v\}^i$

$$\le C'_{d,v}\Big[\prod_{j=1}^{d} \max\{1, |y_j|\}\Big]^i$$

obs. $C'_{d,v} = 1$ if v non archimedean

$$\underset{\|}{h(a_i)}$$

$$\sum_{v \in M_{\mathbb{Q}}} \log^+|a_i|_v \le \sum_{\substack{v \in M_{\mathbb{Q},\infty} \\ j=1 \dots d}} \log(C'_{d,v}) + d\log^+|y_j| + \sum_{v \in M_{\mathbb{Q}} \setminus M_{\mathbb{Q},\infty}} d \log^+|y_j| = d\log(C'_{d,v}) + i\,d\,h(x)$$

$\rightsquigarrow$ finitely many possibilities for a_i ! ///